22 Science and Security in the 21st Century

Commission on Science and Security

Executive Summary

The commission on science and security was asked to assess the new challenges that the Department of Energy (DOE) faces in operating premier scientific institutions in the 21st century while protecting and enhancing national security. In his charge to the commission after taking office, Secretary of Energy Spencer Abraham asked that the commission reject the notion that increased security, by necessity, will diminish the quality of the science carried out at the DOE national laboratories and to look for ways to achieve more of both. Pursuant to its charge, the commission has sought to identify constructive means for meeting this objective. Our key findings and recommendations are set forth below.

The commission's overarching finding is that DOE's policies and practices risk undermining its security and compromising its science and technology programs. In support of its overarching finding, the commission identified five fundamental problems.

First, the Department's continuing management dysfunction impairs its ability to carry out its science and security missions. Even the best security policies and sound processes for their development will not be effective if strong leadership and effective management are lacking. DOE's headquarters, field, contractor, and laboratory relationships create a complicated layered structure in which assigning accountability is difficult. Multiple constituencies mean that internal Department battles consume an inordinate amount of time.

This chapter is reprinted with the permission of the Center for Strategic & International Studies from Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories, *Commission on Science and Security, pp. xii-xx (Executive Summary).*

As a consequence, the development and management of security policy lack clarity, consistency, and broad strategic planning.

Second, collaboration between the science and the security and counterintelligence communities has been badly damaged and must be repaired. The commission found no one from the scientific community who thought it was unimportant to protect national security information. Neither did we find anyone from the security community who felt laboratory scientists did not need to interact with their outside peers. We did find widely differing views on what constitutes a significant risk to national security and how best to minimize those risks. There are deeply held differences dividing the communities over what requires protection, how much protection is needed, and by what means that protection should be provided.

Third, DOE has no effective system for risk-based security management practices. The Department has no system wide approach for assessing risks to its assets and no means for comprehensively determining priorities for the protection of those assets. It also lacks a budget process that could support security decisions based on establishing risk and priorities. Thus, overall spending on security has no underlying rationale, nor does it take into consideration the opportunity costs to science of implementing security measures. In addition, the Department does not have the needed counterintelligence analytical capabilities to support and shape risk-based security management.

Fourth, the Department's investments in new tools and technologies for its security and counterintelligence programs are woefully inadequate. In the last few years, security and counterintelligence have received significant funding increases, but virtually no resources are being devoted to develop systems that move beyond the Department's labor-intensive, paper-based security system. This lack of automation and integration results in missed opportunities to significantly improve the monitoring of processes, facilities, and databases, and bogs down management and scientists under unnecessary administrative burdens.

Finally, cybersecurity lacks sufficient priority in the Department. Management of DOE networks needs significant improvement. More than any other area, cybersecurity demands strong, smoothly

functioning processes to ensure that the laboratories can protect themselves against cyber threats in a manner that is risk based.

The context for these findings and our recommendations is a Department comprising a highly diverse, heterogeneous, and interconnected laboratory system. DOE's three national security laboratories conduct some of the nation's most highly classified research and development in support of maintaining our nuclear deterrent. At the same time, DOE manages a number of other world-class laboratories, most of which conduct no classified work at all. It is crucial to understand that classified work has come to depend on unclassified science and technology, and unclassified science in turn has become more international and connected by advanced communications systems. Accordingly, providing for excellence in both science and security requires increased vigilance and increased threat awareness on the part of the national laboratories, within a risk-based system that will allow open, unclassified scientific interactions to flourish.

Recommendations

To make the necessary changes, the commission believes that the Department must establish a security and counterintelligence program that is sustainable for the long term—one that is risk-based and tailored to the missions and activities of the laboratories. This report suggests five overarching sets of recommendations, the key aspects of which are summarized below. This is followed by a list of all major recommendations.

Recommendation 1
Clarify Lines of Responsibility and Authority

First, if reforms in security and counterintelligence programs are to succeed, the Secretary and the Administrator of the National Nuclear Security Administration (NNSA) must address basic organizational problems at DOE, most significantly confusion over line and staff responsibilities. The commission recommends clarification of the chain of command between the Secretary and the laboratory directors; most important, the responsibility for security, like safety or any

other operational matter, must rest with line management. Together with a more clearly defined chain of command, DOE needs to reduce excess layers of management and staff that have built up since the late 1980s. To support a more disciplined decisionmaking process on all matters, including security, the commission recommends that the Department install a rigorous multiyear budget process, modeled on the planning, programming, and budgeting system (PPBS) at the Department of Defense (DOD). Related to this point, the commission believes that the idea of a separate security budget administered by someone other than the laboratory director as the line manager is a flawed concept, and the commission recommends that line managers control the resources required to execute their missions and supporting operations.

Recommendation 2
Integrate Science and Security

DOE leadership must ensure that science and security at DOE is an integrated enterprise—collaborative and complementary. First, the commission underscores the importance of ensuring that laboratory directors have full responsibility and authority for science and security and of holding the laboratory directors strictly accountable. The laboratory director must be chief scientist and chief security officer. Scientists and engineers throughout each laboratory must be invested in carrying out their missions securely, but this will only happen if laboratory directors themselves take a strong leadership role. Contracts, directives, and other guidance to the laboratories must reflect this philosophy; they must be performance based so that laboratory directors have the capacity to implement them in a manner that is consistent with the work at their sites. At the same time, DOE over-sight must be rigorous and DOE leadership must demand—and reward—accountability. To improve collaboration, the commission also recommends the creation of a high-level, Department-wide laboratory security council for the development of security policies. Its representation should include security, counterintelligence, the field offices, laboratory personnel, and others for whom security policy decisions will have a significant impact. Laboratory directors should

establish comparable groups to integrate security decisionmaking and implementation at the site level. Finally, the Department must take steps to ensure that its counterintelligence program as well as its personnel, cyber, and physical security operations form an integrated system of security that protects and supports the work of the Department. Together with these integration improvements, DOE leadership must restore a climate of trust within the Department, between managers at all levels, and between managers and employees.

Recommendation 3
Develop and Practice Risk-based Security

Third, the Department must develop and practice risk-based security management. Risk-based security management is based on the premise that sensitive activities are not uniformly distributed throughout an organization and that assets representing a higher risk to national security require greater protection. A risk-based system should provide for the ability to make decisions about the marginal value (in an economist's definition, i.e., additional value) of increasing investments in a given aspect of security and the trade-offs between security alternatives, as well as the trade-offs between security and the science (programmatic) mission. The commission believes that a modern security system must find a way to balance resources, which are limited, and risk, which can never be eliminated.

Specifically, the commission recommends the establishment of a risk-based systems approach to the development, analysis, and implementation of security policies throughout the DOE complex. A key to the success of this approach will be clear guidance for the laboratories about the Department's priorities for protecting its assets. That guidance can only be developed with the participation of national security, intelligence, and law enforcement agencies outside DOE. It also will require a greatly improved threat assessment process. The commission recommends that risk-based management plans be developed annually across security functions at each site. In parallel with the budget, the Secretary and the NNSA Administrator should issue a single DOE-wide integrated safeguards and security

plan that reflects the comprehensive plans agreed upon by the sites and federal managers.

To support this risk-based model, the Department needs to strengthen, refocus, and revalidate its counterintelligence program. It is crucial that DOE leadership expand the Department's counterintelligence analytical capabilities in order to conduct pattern analysis, monitor trends, and provide the threat assessments that are necessary for a security system that is properly oriented around risk. The program must broaden its cooperation and information access across agency boundaries and, as discussed in Recommendation 4 below, invest in new technologies. The counterintelligence program should assist in shaping security measures but leave the responsibility for decisions regarding security to line management; its primary function should be collection, investigation, and analysis. In this respect, the com-mission recommends that the counterintelligence program strengthen cooperation with the scientific community for information collection purposes; DOE leader-ship must ensure that counterintelligence officers have access to available information at all laboratories, including the unclassified, open-science laboratories. At the same time, the commission recommends removing unproductive security burdens associated with collecting that information, particularly on unclassified foreign scientific collaboration.

The commission also makes a number of specific recommendations for clarification or amendment to four specific security policies: the so-called zero-tolerance policy, the polygraph program, practices for controlling sensitive unclassified information, and the policies affecting fundamental research.

Recommendation 4
Adopt New Tools and Techniques

DOE must augment its capabilities for security and counterintelligence with significant investment in new tools and techniques. Specifically, DOE must develop and invest in state-of-the-art technologies for personnel authentication, access control to cyber systems and facilities, and data fusion and analysis techniques. The Department should be investing in biometric and other systems that would help

make authentication and access control processes more robust and less intrusive. By employing new technologies, DOE could strengthen positive identification of employees and visitors and significantly reduce cumbersome physical and cyber access requirements. In parallel, DOE also must invest in databases, information systems, and analytical tools to perform data cross-correlation, data mining, and other analysis for security and counterintelligence purposes. Such tools are badly needed in order to strengthen the analytical capacity of the counterintelligence program.

Recommendation 5
Strengthen Cybersecurity

DOE must devote priority attention to strengthening cybersecurity; it is both the strength and the Achilles' heel of the scientific enterprise. Other parts of this report contain recommendations that would improve cybersecurity, and the commission makes several additional recommendations that are specific to cybersecurity. First, the role of the chief information officer (CIO) in DOE and NNSA should be strengthened by ensuring that the CIO has responsibility for cybersecurity, so that development of cybersecurity policies are integrated with information technology systems policy. DOE should also establish a cybersecurity advisory panel that uses the knowledge and experience of outside experts to bring cutting-edge solutions to the DOE cyberenterprise. Finally, DOE must place a higher priority on the timely implementation of cybersecurity solutions that are already developed and do more to evaluate emerging technologies being developed by other agencies and the private sector.

List of Recommendations

DOE leadership (the Secretary, Deputy Secretary, NNSA Administrator, and the Under Secretary for Energy, Science, and Environment, as appropriate) should undertake the following steps:

Recommendation 1
Clarify Lines of Responsibility and Authority

- Clarify line management and staff responsibilities.
- Clarify federal policymaking and oversight responsibilities.
- Reduce the size of the federal staff.
- Commit to the government-owned, contractor-operated (GOCO) model of management.
- Build an integrated, multiyear budgeting process.
- Assign a single point of responsibility for counterintelligence.

Recommendation 2
Integrate Science and Security

Embed security in the science mission:

- Make implementation of the integrated safeguards and security management (ISSM) policy a top priority.
- Ensure laboratory directors have full responsibility and authority for science and security at their sites, and are held accountable.
- Clarify that security and counterintelligence professionals must provide staff support to line management, at all levels of the system.
- Revise directives and other guidance to the laboratories so that they are performance based instead of compliance oriented.

- Ensure that the laboratories are subject to rigorous oversight.

- Institute development of a service approach to security management for the laboratories.

Strengthen collaboration among science, security, and counterintelligence elements:

- Establish a laboratory security council, chaired by the Deputy Secretary, to provide for the collaborative development of security policies.

- Direct that laboratory directors establish an integrated security group at each site to provide for collaborative implementation of security policies.

- Institute an annual DOE-wide implementation conference to share best practices and address crosscutting problems.

- Establish a program to detail security, counterintelligence, and science professionals on a rotational basis to DOE headquarters and the laboratories.

- Require regular interaction between top DOE management and laboratory directors on security issues.

Strengthen coordination across security and counterintelligence functions:

- Establish close coordination at headquarters across security and counterintelligence functions.

- Request that laboratory directors establish teams comprising counterintelligence and security elements at each site.

Restore a climate of trust:

- Clarify security expectations for line management with respect to their leadership roles and responsibilities on security matters.

- Make security expectations for employees clear, logical, and appropriate to the task.

Recommendation 3
Develop and Practice Risk-based Security

Develop and implement a risk-based security model:

- Develop a risk-based systems approach to managing security for the DOE complex, to be implemented through integrated teams at headquarters and the laboratories.

- Provide overarching guidance from headquarters to the sites for the development of integrated safeguards and security plans, including high-level priorities for assets requiring protection.

- Direct the laboratories to conduct annual integrated safeguards and security risk assessments and develop plans at the site level, through integrated risk management teams.

- In parallel with the budget, issue an annual DOE enterprise-wide safeguards and security plan comprising the individual laboratory plans.

Strengthen, refocus, and revalidate counterintelligence:

- Expand significantly the analytical capabilities of counterintelligence to collect, fuse, and analyze data from all sources.

- Relieve the counterintelligence program of its perceived responsibility for acting as a security regulator; encourage the counterintelligence program to strengthen cooperation with the scientific community for information collection and analytical purposes.

- Revise policy for foreign unclassified visits to ensure sound data collection, but also allow laboratory directors to exercise judgment regarding advance screening requirements.

- Ensure that counterintelligence officers have the necessary access to information on foreign nationals at the unclassified, open-science laboratories.

- Establish local arrangements between counterintelligence officers and scientists regarding cooperative research and development agreements (CRADAs).

- Request a National Security Council–led review of Presidential Decision Directive 61 (PDD-61) to ensure its interpretation is consistent with the commission's recommendations, and revise it as necessary.

Amend and clarify security practices:

- Issue a comprehensive statement of security policy and principles that authoritatively defines the zero-tolerance policy by leaving room for reasoned judgment, within the context of maintaining rigorous security.

- Implement a polygraph policy comparable to that of the Department of Defense (polygraph examinations chiefly used as an investigative tool; sparingly as a screening tool when exceptional program security is needed).

- Amend policies dealing with sensitive unclassified information:

  - Streamline and simplify policies for sensitive unclassified information by discontinuing the use of sensitive unclassified definitions and labels;
  - Direct all laboratories to undertake a systematic review to ensure proper control of classified information under existing guidelines;
  - Direct a review of unclassified information not currently subject to statutory administrative controls for possible placement under a single administrative control category of official use only (OUO); and

- Ensure close cooperation between counterintelligence officials and the laboratories when a specific concern arises regarding unclassified information.

- Seek reissuance of President Reagan's National Security Decision Directive 189 (NSDD-189) to reaffirm that fundamental research is generally exempt from security regulations and that any controls can be imposed only through a formal process established by those regulations.

Recommendation 4
Adopt New Tools and Techniques

Develop and acquire state-of-the-art security and counterintelligence technologies:

- Invest in new technologies, such as public key infrastructure (PKI) and biometric systems for access to all cyber systems and for access to all sensitive facilities.

- Invest in databases, information systems, and analytical tools to perform extensive fusion, analysis, and data mining of authorization, access, biometric, counterintelligence, and related data.

- Establish processes for applying the above tools and techniques to the visitor request, approval, and monitoring system for visitors to DOE laboratories.

Augment analytic and advisory capabilities for security and counterintelligence:

- Establish for a limited time a small, independent technical team outside DOE (e.g., at a federally funded research and development center) to help develop and refine a risk-based integrated security model.

- Establish a standing security advisory board.

Recommendation 5
Strengthen Cybersecurity

- Assign the chief information officers for DOE and NNSA the lead responsibility for cybersecurity.

- Establish a high-level cybersecurity advisory panel.

- Establish standard operating procedures, appropriate to each laboratory, to measure and provide oversight of cyber network performance.

- Implement classified cyber systems rapidly at DOE headquarters.

- Ensure that developed cybersecurity solutions are implemented with high priority and that emerging technologies are evaluated for possible use.